



IT Security Handbook

System and Service Acquisition -

ITS-HBK-2810.05-01 -
Effective Date: 20110506 -
Expiration Date: 20130506 -
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.05-01)
System and Service Acquisition


Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

Change History	2 -
1 Introduction and Background	4
2 Allocation of Resources (SA-2)	5
3 Life Cycle Support (SA-3)	5
4 Acquisitions (SA-4)	5
5 Information System Documentation (SA-5)	6
6 Software Usage Restrictions (SA-6)	6
7 User-Installed Software (SA-7)	6
8 Security Engineering Principles (SA-8)	6
9 External Information System Services (SA-9)	6
10 Developer Configuration Management (SA-10)	6
11 Developer Security Testing (SA-11)	6
12 Supply Chain Protection (SA-12)	6
13 Trustworthiness (SA-13)	7
14 Organizationally Defined Values	8

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's System and Service Acquisition (SA) information security controls.
- 1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 - The System and Services Acquisition control family relates to the need to adequately plan for, appropriately fund, and efficiently acquire the resources necessary to maintain information security. The control family defines the actions that best enable NASA's security program to make effective use of externally-sourced expertise and tools. Furthermore, it mandates that security considerations not be treated as an afterthought, but are instead addressed early-on in parallel with funding and design decisions.
- 1.7 - **Applicable Documents**
- *NASA Federal Acquisitions Regulation (FAR) Supplement*
 - *NPD 2810.1, NASA Information Security Policy*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements*
 - *ITS-HBK-2810.02-05, Security Assessment and Authorization: External Information Systems*
 - *ITS-HBK-2810.03-02, Planning: Information System Security Plan Template, Requirements, Guidance and Examples*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-23, Guide to Federal Organizations on Security Assurance and Acquisition*
 - *NIST SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
 - *NIST SP 800-30, Risk Management Guide for Information Technology Systems*
 - *NIST SP 800-34, Contingency Planning Guide for Information Technology Systems*
 - *NIST SP 800-35, Guide to Information Technology Security Services*
 - *NIST SP 800-36, Guide to Selecting Information Technology Security Products*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
 - *NIST SP 800-39, Managing Risk from Information Systems: An Organizational Perspective*

ITS Handbook (ITS-HBK-2810.05-01) -
System and Service Acquisition -

- *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
- *NIST SP 800-60, Guide for Mapping Types of Information and Information Systems*
- *NIST 800-64, Security Considerations in the System Development Lifecycle*
- *NIST SP 800-70, National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*

2 Allocation of Resources (SA-2)

2.1 - Roles and Responsibilities

- 2.1.1 *The Center Chief Information Officer (CIO) shall: -*
 - 2.1.1.1 - Ensure that Exhibit 300 submissions correctly list all information system security requirements. -
- 2.1.2 *The Information System Owner (ISO) shall: -*
 - 2.1.2.1 - Determine and document information system security requirements. -
 - 2.1.2.2 - Submit information system security requirements for inclusion in NASA capital planning and investment control - processes. -
 - 2.1.2.2.1 Requirements shall exist as discrete line items in the information system Exhibit 300. -
 - 2.1.2.3 - Allocate garnered resources to ensure the security of the information system. -
- 2.1.3 *The Information System Security Officer (ISSO) shall: -*
 - 2.1.3.1 - Advise and assist the ISO on information system security requirements and their documentation. -

3 Life Cycle Support (SA-3)

- 3.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security - categorization and risk environment of the information and/or information system. -

4 Acquisitions (SA-4)

4.1 - Roles and Responsibilities

- 4.1.1 *The Agency Contracting Office (CO) responsible for the solicitation shall: -*
 - 4.1.1.1 - Ensure solicitation and acquisition contracts correctly include documented information system security - requirements. -
 - 4.1.1.2 - Ensure the inclusion of *NASA FAR Supplement 1852.204-76, NASA IT Security Clause* in all solicitation and - acquisition contracts. -
- 4.1.2 *The Local Contracting Office Technical Representative (COTR) shall: -*
 - 4.1.2.1 - Ensure that contractor systems and services implement security requirements prescribed by, and provide the - reports and documentation required by the *NASA FAR Supplement 1852.204-76, NASA IT Security Clause*. -
 - 4.1.2.2 - Require that contractors and vendors provide information describing the functional properties of the security - controls to be employed as a part of the contracted information system or service in sufficient detail to permit - analysis and testing. -
 - 4.1.2.3 - Require that every information system component acquired is associated with an information system, and that the - owner of the information system is aware of the association. -
- 4.1.3 *The ISO shall: -*
 - 4.1.3.1 - Ensure detailed information system requirements are documented prior to selection and acquisition, in a manner - consistent with *NPR 7120.7*. -

5 Information System Documentation (SA-5)

5.1 - Roles and Responsibilities

5.1.1 *The ISO shall:* -

5.1.1.1 - Ensure that the policies and procedures documented in *ITS-HBK-2810.03-02* are followed. -

6 Software Usage Restrictions (SA-6)

6.1 - Roles and Responsibilities

6.1.1 *The ISO shall:* -

6.1.1.1 - Document and inventory all software installed on information systems in related documentation (e.g. System - Security Plan) through NSAAR. -

7 User-Installed Software (SA-7)

7.1 - Roles and Responsibilities

7.1.1 *The ISO shall:* -

7.1.1.1 - Document and inventory all software installed on information systems in related documentation (e.g. System - Security Plan) through NSAAR. -

7.1.2 *The NASA User shall:* -

7.1.2.1 - Adhere to the requirements of the Rules of Behavior for their system. -

7.1.2.2 - Not install software whose pedigree, with regard to being potentially malicious, is unknown or suspect. -

8 Security Engineering Principles (SA-8)

8.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security - categorization and risk environment of the information and/or information system. -

9 External Information System Services (SA-9)

9.1 - Roles and Responsibilities

9.1.1 *The AO shall:* -

9.1.1.1 - Approve the acquisition or outsourcing of dedicated information security services. -

9.1.2 *The ISO shall:* -

9.1.2.1 - Ensure the policies and procedures documented in *ITS-HBK-2810.02-05* are followed. -

10 Developer Configuration Management (SA-10)

10.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security - categorization and risk environment of the information and/or information system. -

11 Developer Security Testing (SA-11)

11.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security - categorization and risk environment of the information and/or information system. -

12 Supply Chain Protection (SA-12)

12.1 - Roles and Responsibilities

12.1.1 *The ISO shall:* -

12.1.1.1 - Determine the level of risk to an information system related to the information which is necessarily disclosed to - vendors and suppliers during the acquisition process. -

- 12.1.1.2 Ensure the inclusion of spare information system components in the initial acquisition in a manner consistent with the cost and risk associated with the information system.

13 Trustworthiness (SA-13)

13.1 Roles and Responsibilities

13.1.1 *The ISO shall:*

- 13.1.1.1 Ensure that implemented security controls are implemented correctly, operating as intended, and producing valid results in a manner consistent with organizationally defined values.

14 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

800 53 Reference							FIPS 199 Categorization		
Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
SA	01	System and Services Acquisition Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
SA	09	External Information System Services	E 1	[1]	Reference	Approving official for the acquisition or outsourcing of dedicated information security services.	Authorizing Official	Authorizing Official	Authorizing Official
SA	12	Supply Chain Protection	Main	[1]	Reference	List of measures to protect against supply chain threats.			1. Purchase critical system spares and components in the initial acquisition. 2. Use standard configurations to maximum extent possible for components and IT products.

ITS Handbook (ITS-HBK-2810.05-01) -
System and Service Acquisition -

800 53 Reference							FIPS 199 Categorization		
Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
SA	13	Trustworthiness	Main	[1]	Reference	Level of trustworthiness required of an information system.			High - Requires security functionality and security assurance testing and validation.